

REMARKS

Claims 1, 6, 8, and 11 have been amended. Claims 3, 4, and 12 have been cancelled.

Claims 1-2, 5-11, and 13-14 remain in the case.

1. Amendments to Claims 1, 6, 8, and 11

Claims 1, 6, 8, and 11 have been amended, in a somewhat similar manner, to more clearly define the present invention in one or more embodiments. Claim 1 for example, now specifies:

1. A method comprising the steps of:
 - encrypting a data message m using a primary transmitter secret key z to form a quantity E , ~~wherein El Gamal encryption is used for encrypting the data message m ;~~
 - preparing a quadruplet $(a_{\text{new}}, b_{\text{new}}, s_{\text{new}}, E)$ where:
 - $a_{\text{new}} = z * y^c \text{ modulo } p$;
 - $b_{\text{new}} = g^c \text{ modulo } p$;
 - $s_{\text{new}} = \text{signature}_c(a_{\text{new}}, b_{\text{new}}, E)$;
 - where $y = g^x \text{ modulo } p$, ~~c is a random number which is used in the step of encrypting the data message m using El Gamal encryption~~, x is a receiver secret key, and the parameters g , x , and p are picked using a known encryption method;
 - wherein s_{new} is a signature which is determined by using the same random number c that was used to determine a_{new} and b_{new} ;
 - verifying the signature s_{new} ;
 - decrypting a_{new} and b_{new} using the receiver secret key x to get the primary transmitter secret key z ;
 - using the primary transmitter secret key z to decrypt the quantity E and thereby obtaining the message m .

In the present application El Gamal encryption is used in one embodiment. (Present application, pg. 7, fourth paragraph – pg. 8, second paragraph). In one embodiment, a random number “ c ” used in the El Gamal encryption is also used to determine a signature. (Present application, pg. 7, fourth paragraph – pg. 8, second paragraph).

It is respectfully submitted that the prior art does not suggest using El Gamal encryption, with a specific random number “ c ” and then performing a signing process using the same random number “ c ”.

For at least the above reasons or similar reasons, claims 1, 6, 8, and 11 are respectfully submitted to be allowable. Claims 2, 5, and 9-10 are dependent on claim 1, claim 7 is dependent

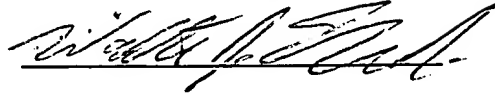
on claim 6, and claims 13 and 14 are dependent on claim 11, and therefore these claims are also submitted to be allowable for at least the same or similar reasons.

2. Conclusion:

In view of the foregoing, the remaining claims in the case, claims 1-2, 5-11, and 13-14 are submitted to be allowable. Favorable reconsideration of this application, as amended, is respectfully requested. A credit card payment form for \$770.00 for a request for continued examination is enclosed.

DATED: 3/24/04

Respectfully submitted,



Walter J. Tencza Jr.
Reg. No. 35,708
10 Station Place, Suite 3
Metuchen, N.J. 08840
Phone: 732- 549-3007
Fax: 732-549-8486